

## CLAIMS:

What is claimed is:

1. A method for providing secure access to console functions of a computer system comprising:
  - initiating a first EKE sequence to generate a device shared secret utilizing a default device identifier and associated shared secret on a system-attached device from which a console operation is desired enabled;
  - generating said device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and
  - storing said device shared secret within a storage location of said system and on said system-attached device.
2. The method of Claim 1, wherein said shared secret is stored in a protected manner on said system-attached device and utilized with a device ID during each connection of said system-attached device to said system.
3. The method of Claim 2, further comprising encrypting operator authentication data flowing between said system-attached device and said system utilizing said shared secret.
4. The method of Claim 2, method further comprising encrypting operator authentication data flowing between said system-attached device and said system utilizing a hash of said shared secret.

1           5.     The method of Claim 2, further comprising:  
2                 responsive to an establishment of a first console session that authenticates said  
3           system-attached device, instantiating a second EKE sequence to authenticate a  
4           console operator utilizing a default user identifier and password; and  
5                 storing said user identifier and password in a protected area of said storage  
6           location of said system.

1           6.     The method of Claim 5, further comprising:  
2                 enabling a setup of multiple device identifiers and authorization levels for  
3           other system-attached devices to act as console devices; and  
4                 storing said multiple device identifiers and authorization levels in said storage  
5           location.

1           7.     The method of Claim 5, further comprising:  
2                 enabling a setup of multiple operator user identifiers and associated passwords  
3           and authorization levels for other console operators to access console functions of the  
4           system; and  
5                 storing said multiple operator user identifiers and associated passwords and  
6           authorization levels in said storage location.

1           8.     The method of Claim 5, further comprising enabling multiple console sessions  
2           for different systems on a single console device.

1           9.     A system for providing secure access to console functions of a computer  
2           system comprising logic for:  
3                 initiating a first EKE sequence to generate a device shared secret utilizing a  
4           default device identifier and associated shared secret on a system-attached device  
5           from which a console operation is desired enabled;

6           generating said device shared secret from said first EKE sequence, wherein  
7           said device shared secret is utilized in place of said default device shared secret in  
8           subsequent console authentication procedures; and

9           storing said device shared secret within a storage location of said system and  
10          on said system-attached device.

1           10.    The system of Claim 9, wherein said shared secret key is stored in a protected  
2           manner on said system-attached device and utilized as a device ID during each  
3           connection of said system-attached device to said system.

4           11.    The system of Claim 10, further comprising encrypting operator  
5           authentication data flowing between said system-attached device and said system  
6           utilizing said shared secret.

7           12.    The system of Claim 10, method further comprising logic for encrypting  
8           operator authentication data flowing between said system-attached device and said  
9           system utilizing a hash of said shared secret.

10          13.    The system of Claim 10, further comprising logic for:  
11          responsive to an establishment of a first console session that authenticates said  
12          system-attached device, instantiating a second EKE sequence to authenticate a  
13          console operator utilizing a default user identifier and password; and  
14          storing said user identifier and password in a protected area of said storage  
15          location of said system.

1           14.    The system of Claim 13, further comprising logic for:  
2           enabling a setup of multiple device identifiers and authorization levels for  
3           other system-attached devices to act as console devices; and

4 storing said multiple device identifiers and authorization levels in said storage  
5 location.

1 15. The system of Claim 13, further comprising logic for:  
2 enabling a setup of multiple operator user identifiers and associated passwords  
3 and authorization levels for other console operators to access console functions of the  
4 system; and  
5 storing said multiple operator user identifiers and associated passwords and  
6 authorization levels in said storage location.

1 16. The system of Claim 13, further comprising logic for enabling multiple  
2 console sessions for different systems on a single console device.

1 17. A computer program product comprising:  
2 a computer readable medium; and  
3 program code on said computer readable medium for providing secure access  
4 to console functions of a computer system by:  
5 initiating a first EKE sequence to generate a device shared secret utilizing a  
6 default device identifier and associated shared secret on a system-attached device  
7 from which a console operation is desired enabled;  
8 generating a device shared secret from said first EKE sequence, wherein said  
9 device shared secret is utilized in place of said default device shared secret in  
10 subsequent console authentication procedures; and  
11 storing said device shared secret within a storage location of said system and  
12 on said system-attached device.

1 18. The computer program product of Claim 17, wherein said shared secret key is  
2 stored in a protected manner on said system-attached device and utilized as a device  
3 ID during each connection of said system-attached device to said system.

1 19. The computer program product of Claim 18, further comprising program code  
2 for encrypting operator authentication data flowing between said system-attached  
3 device and said system utilizing said shared secret.

1 20. The computer program product of Claim 18, further comprising program code  
2 for encrypting operator authentication data flowing between said system-attached  
3 device and said system utilizing a hash of said shared secret.

1 21. The computer program product of Claim 18, further comprising program code  
2 for:

3 responsive to an establishment of a first console session that authenticates said  
4 system-attached device, instantiating a second EKE sequence to authenticate a  
5 console operator utilizing a default user identifier and password; and

6 storing said user identifier and password in a protected area of said storage  
7 location of said system.

1 22. The computer program product of Claim 21, further comprising program code  
2 for:

3 enabling a setup of multiple device identifiers and authorization levels for  
4 other system-attached devices to act as console devices; and

5 storing said multiple device identifiers and authorization levels in said storage  
6 location.

1           23.    The computer program product of Claim 21, further comprising program code  
2           for:

3                    enabling a setup of multiple operator user identifiers and associated passwords  
4           and authorization levels for other console operators to access console functions of the  
5           system; and

6                    storing said multiple operator user identifiers and associated passwords and  
7           authorization levels in said storage location.

1           24.    The computer program product of Claim 21, further comprising program code  
2           for enabling multiple console sessions for different systems on a single console  
3           device.

4           25.    A method of signing in authenticated users to a console function of a system,  
5           comprising:

6                    determining via a first EKE sequence whether a device identifier and  
7           associated shared secret of a system-attached device matches a stored device identifier  
8           and associated shared secret on said system;

9                    responsive to both ends having identical shared secrets, receiving a user-  
10          entered identifier and password;

11                   responsive to said receiving, initiating a second EKE sequence to determine  
12          whether said user-entered identifier and password matches a user identifier and  
13          password combination stored on a storage location of said system; and

14                   granting said user access to console functions only when said second EKE  
15          sequence is successful.

1           26.    The method of Claim 25, further comprising encrypting data transmitted  
2           during said second EKE sequence utilizing a shared secret generated during said first  
3           EKE sequence.

1           27.     A method for secure authentication of a system console device within a  
2     network environment, comprising:

3                 establishing a first console session from an authentication device, wherein a  
4     default device identifier is utilized to initiate an EKE sequence between a network-  
5     attached console device and a..

6                 generating a shared secret key via an EKE sequence utilized to establish said  
7     first console session; and

8                 subsequently authenticating a console operator via a second EKE sequence,  
9     wherein said shared secret key is utilized to encrypt data of an authentication process  
10    for said console operator attempting to utilize said console operation.